IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

MARC OPPERMAN, *et al*., for themselves and all others similarly situated,	§	
	§	
Plaintiffs,	§	**CASE NO. 1:12-cv-00219-SS**
	§	
v.	§	
	§	
PATH, INC., *et al.*,	§	
	§	
Defendants.	§	

DEFENDANT TWITTER, INC.'S MOTION TO DISMISS UNDER RULES 12(b)(6) AND 12(b)(3) OR 12(b)(1)

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BACKGROUND 2

III. ARGUMENT 3

A. Plaintiffs Do Not Have Article III Standing 3

B. Plaintiffs Fail to Allege that Twitter Acted Wrongfully or Without Consent 5

C. Plaintiffs Fail to Adequately Allege the Common Law and State Statutory Claims 5

a. Invasion of Privacy 5

b. Theft 7

c. Conversion and Trespass to Chattels 7

d. Computer Hacking, Cal. Penal Code § 502 8

e. Negligence, Negligence Per Se, and Gross Negligence 8

f. Common Law and Trade Secret Misappropriation 10

g. Unjust Enrichment 11

h. Constructive Trust 11

i. Wiretap Claims Under California and Texas Law 12

D. Plaintiffs Fail to Adequately Allege the Statutory Claims Under Federal Law 12

1. Electronic Communications Privacy Act ("ECPA") 12

a. Plaintiffs have not alleged an interception 12

b. Plaintiffs have not alleged use of an interception device, and any alleged interception would have been in the ordinary course of Twitter's providing its Find Your Friends feature 13

c. Plaintiffs have not alleged wrongful use or disclosure 14

TABLE OF CONTENTS
(continued)

Page

2. 18 U.S.C. § 1030(g), Computer Fraud and Abuse Act ("CFAA") 14

a. Plaintiffs have not alleged a specific claim under the CFAA 14

b. Plaintiffs have not sufficiently alleged a statutory prerequisite under Sections 1030(g) and 1030(c)(4)(A)(i) 15

c. Plaintiffs have not alleged Twitter acted without authorization or exceeded authorized access 16

E. Plaintiffs Have Failed to Adequately Allege the RICO Claim 17

F. This Court Should Dismiss Plaintiffs' Action Pursuant to Rule 12(b)(3) or 12(b)(1) 19

IV. CONCLUSION 20

I. INTRODUCTION

Defendant Twitter, Inc. operates a service that allows friends, family, and co-workers to communicate and stay connected through the exchange of quick, short messages called "Tweets." Users can choose to subscribe to the Tweets of another user, otherwise referred to as "following" the user. Twitter assists its users in finding those people they want to "follow" by offering a "Find Your Friends" feature in the Twitter mobile application ("app"). Plaintiffs chose to activate this feature and acknowledge that when they did so, Twitter expressly told them it would scan their mobile contacts to do exactly what was described: help find their friends.

Plaintiffs now include Twitter in their multi-defendant Second Amended Complaint ("SAC") because, they allege, the defendants as a whole "uploaded" the "private address books" of consumers in an unauthorized manner, and they seek class action status against all of the defendants. However, in the case specifically directed at Twitter, it is beyond dispute that plaintiffs consented to Twitter's access to and use of plaintiffs' contacts in order to match them with other Twitter users. Further, plaintiffs have not plausibly alleged that their contacts were used in any unauthorized fashion or not securely transmitted by Twitter, or that plaintiffs were damaged by Twitter's actions. Plaintiffs attempt to ignore Twitter's Terms of Service, in which all users of the app (including plaintiffs) consent to Twitter's uploading and use of their contacts, and agree that any complaint such as plaintiffs' must be brought in California.

Plaintiffs improperly[1] lump together Twitter and 15 other defendants in an effort to paint them all with a broad brush, hoping that—simply because the defendants' apps were distributed through the Apple App Store and ran on Apple mobile devices, and some defendants allegedly did a poor job obtaining consent to access users' contacts—there must be actionable wrongdoing by all of them. Plaintiffs have failed to state any claim against Twitter, however, and the Court should therefore dismiss this action against Twitter. And even if there is a claim, plaintiffs failed to bring it in the proper forum, and the Court should dismiss Twitter from this action.

[1] Twitter has concurrently filed a Motion to Sever.

II. BACKGROUND

In an 83-page, 439-paragraph Complaint that manages to say little of substance against Twitter, 14 individual plaintiffs have sued 16 defendants based on their separate interactions with 11 different applications.[2] As a general matter, plaintiffs complain that each application accessed and used their "address book data" (loosely defined as some combination of names, email addresses, phone numbers, addresses, and other information) from plaintiffs' iPhones, iPads, and iPod Touches (collectively "Apple Devices"). (*See, e.g.*, SAC ¶¶ 165, 190, 220, 254, 362.) Plaintiffs bring federal causes of action under the Computer Fraud and Abuse Act ("CFAA"), the Wiretap Act, and the Racketeer Influenced and Corrupt Organizations ("RICO") Act (alleging wire fraud and transportation of stolen property as predicate acts). They assert violations of California and Texas laws regarding wiretaps and wrongful access to computers, and state torts including negligence, conversion, invasion of privacy, and trespass to chattels.

With respect to Twitter, plaintiffs allege they signed up for Twitter's service, a public microblog that allows users to "Tweet" messages in 140 characters or less and to follow others' "Tweets." (SAC ¶ 232.) Plaintiffs concede that, when signing up for Twitter, they chose to use Twitter's "Find Your Friends" feature. (SAC ¶ 232.) They further concede that they were told that using the feature meant Twitter would scan their contacts on their Apple Device. (*See, e.g.*, SAC ¶¶ 232, 165, 190, 220, 254, 362.) Despite this admission, plaintiffs now claim Twitter acted without permission by accessing their address books—specifically, they allege that the service "silently made a call" to upload data to Twitter's servers where it was to be "used, stored and kept for up to eighteen months." (SAC ¶ 235.) Plaintiffs also allege, without support, that Twitter "likely" maintained data "in unsecure plain text." (SAC ¶ 235.)

With the exception of Apple, the only connection between Twitter and each defendant is that each is alleged to be or to own an App Developer, and to provide an application used on

[2] Twitter also joins in the motion for dismissal under Rule 8(a) filed by defendant Zeptolab [Dkt. 110], and adopts the arguments therein. Plaintiffs continue to violate the "short and plain statement" rule, and have violated the Court's order to file a complaint that complies with Rule 8(a). *See* Order of Aug. 23, 2012, Dkt. 99.

Apple Devices. (SAC ¶¶ 24-39). Despite the fact that each App Developer offered a different application and different disclosures, plaintiffs allege that they suffered the same harm from each—the invasion of their privacy and other unspecified harms and costs associated with supposed unwanted access and disclosure. (*See, e.g.*, SAC ¶¶ 81-83, 165, 190, 220, 254, 362.) Plaintiffs allege Apple is complicit in this conduct by providing the apps through their App Store and "teaching" App Developers how to access address book information. (*See, e.g.*, SAC ¶ 133.)

Plaintiffs conspicuously avoid referring to Twitter's terms of service and privacy policy ("Terms").[3] Each Twitter user must create an account and accept the Terms prior to use. (*See* Declaration of Sung Hu Kim in Support of Twitter, Inc.'s Motion to Dismiss ("Kim Decl."), ¶¶ 2-4, Exs. A, B.) The Terms tell users that they may share, and Twitter may collect, information "from your address book so that we can help you find users you know." The Terms also contain a forum selection clause placing exclusive venue in San Francisco, California.[4]

III. ARGUMENT

A. Plaintiffs Do Not Have Article III Standing

The SAC is devoid of facts that would show each plaintiff suffered a concrete, particularized, actual, and imminent injury-in-fact. Further, given their express consent to the very conduct by Twitter of which they now complain, plaintiffs cannot possibly satisfy the requirement that their alleged injury be fairly traceable to Twitter's actions. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

---

[3] "In deciding a motion to dismiss, courts may consider the complaint, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, such as documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Joe W. & Dorothy Dorsett Brown Found. v. Frazier Healthcare V, L.P.*, No. A-11-CA-807-SS, 2012 WL 3834029, at *2 (W.D. Tex. Aug. 27, 2012) (Sparks, J.); *see also Funk v. Stryker Corp.*, 631 F.3d 777, 783 (5th Cir. 2011) (same). This "prevent[s] plaintiffs from surviving a Rule 12(b)(6) motion by deliberately omitting . . . documents upon which their claims are based." *Swartz v. KPMG LLP*, 476 F.3d 756, 763 (9th Cir. 2007). Moreover, on a Rule 12(b)(3) motion, the Court may consider evidence relevant to the forum selection clause. *Ambraco, Inc. v. Bossclip B.V.*, 570 F.3d 233, 238 (5th Cir. 2009).

[4] Plaintiffs allege that they signed up using the Twitter app for Apple Devices, *see* SAC ¶ 232, which was first released in May 2010. (Kim Decl. ¶¶ 3, 8, 9, 11). Twitter's Terms, to which plaintiffs agreed, have contained a forum selection clause and explanation of how address book information may be collected since 2009. (Kim Decl. ¶¶ 8, 9, 11; Exs. D-I, K-O).

In Article III, the U.S. Constitution sets a "hard floor of . . . jurisdiction that cannot be removed by statute." *Summers v. Earth Island Inst.*, 555 U.S. 488, 497 (2009). The first requirement of this "irreducible constitutional minimum" is "an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560-61. This injury "may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing . . . .' [T]he plaintiff still must allege a distinct and palpable injury to himself." *Warth v. Seldin*, 422 U.S. 490, 500-01 (1975) (quoting *Linda R.S. v. Richard D.*, 410 U.S. 614, 61, n.3 (1973)).

An injury in *law*, even if properly alleged, cannot satisfy the constitutional requirement that plaintiffs must have suffered an injury in *fact*. Plaintiffs do not plead facts establishing they sustained a concrete injury-in-fact because of Twitter's acts or omissions. Plaintiffs assert only that they had some ambiguous (and inherently conflicting) privacy or commercial rights in their address books and to their phones' performance, somehow completely undiminished by apps and features the plaintiffs chose to use on their devices, without any support for these creative propositions. (*See* SAC ¶¶ 77-83) (alleging theoretical loss of commercial value while also trying to claim they would keep the data private, a general de-privatizing of data, generalized diminished device resources, and overpayment for Apple Devices resulting in "various harms"); *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008) (holding posting of personal information on the Internet and exposure to risk of access and to future acts of identity theft is "somewhat 'hypothetical' and 'conjectural'" and only actual financial injuries were an injury in fact). Put simply, plaintiffs fail to offer any facts to support their contention that an upload of address book information (that they agreed to let Twitter review) actually impacted them or their devices. *See In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y.) (rejecting contention that collection of personal information is an economic loss to plaintiffs); *LaCourt v. Specific Media*, No. SACV 10-1256-GW, 2011 WL 1661532, at *4 (C.D. Cal. Apr. 28, 2011) (same).[5]

[5] Twitter also adopts the other defendants' arguments regarding plaintiffs' lack of Article III standing.

B. Plaintiffs Fail to Allege that Twitter Acted Wrongfully or Without Consent

The second overarching failure in the Complaint is that plaintiffs base their claims against Twitter on *something that they admit they asked Twitter to do*. Plaintiffs concede they asked Twitter to help them find their friends, and that Twitter disclosed that the "Find Your Friends" feature would scan their contacts. (SAC ¶¶ 231-232.) Plaintiffs try to slip by this problem by asserting that they consented to a "scan" but not an "upload." Plaintiffs not only fail to show how these terms are materially different, they simply ignore that their request to have Twitter scan their contacts and match them with other Twitter users *necessarily* required Twitter to upload contact data and cross reference it against data in Twitter's possession relating to *other* Twitter account holders. Such a consented-to matching process could not possibly occur in the physical confines of plaintiffs' cell phones: whether it is called "scanning" or "uploading," contact data necessarily had to move from plaintiffs' phones to Twitter servers.

Plaintiffs' feigned misunderstanding and strained distinction also ignore Twitter's Terms, conspicuously omitted from the SAC, which explain that Twitter collects address book data to permit users to find friends already on Twitter. (Kim Decl., ¶¶ 9, 11, Exs. D-I, K-O.)

C. Plaintiffs Fail to Adequately Allege the Common Law and State Statutory Claims

Plaintiffs rely on allegations against other defendants to rope Twitter into this lawsuit on "threadbare recitals of the elements of a cause of action, supported by mere conclusory statements," *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (U.S. 2009). If the Court does not dismiss Twitter as a defendant for lack of Article III injury, it should dismiss the claims for failure to state a claim on which relief can be granted, for the reasons below.[6]

a. Invasion of Privacy

Plaintiffs claim Twitter "intruded on [their] solitude, seclusion [or] private affairs," and that such "intrusion" was "highly offensive to a reasonable person," but they fail to plead facts showing an intrusion or that any intrusion was unreasonable, unjustified, or unwarranted. *See Valenzuela v. Aquino*, 853 S.W. 2d 512, 513 (Tex. 1993) (stating elements for invasion of

[6] The standards for dismissal under Rule 12(b)(6) are known to the Court and set out in the Application Developer Defendants' Joint Motion to Dismiss.

privacy by intrusion); *Doe v. Mobile Video Tapes*, 43 S.W.3d 40, 48 (Tex. App.-Corpus Christi 2001, no pet.) (intrusion must be unreasonable, unjustified, or unwarranted to be "highly offensive"); *Miller v. Nat'l Broadcasting Co.*, 187 Cal. App. 3d 1463, 1482 (Cal. App. Ct. 1986) (intrusion must be highly offensive).[7] A "highly offensive act," requires a degree of offensiveness like that of the outrageousness standard for intentional infliction of emotional distress, *see Polansky v. Sw. Airlines Co.*, 75 S.W.3d 99, 105 (Tex. App.-San Antonio 2002, no pet.), and typically involves acts such as videotaping a bedroom without permission, searching a personal locker or purse, and spying and harassment. *See, e.g., Aldridge v. Sec'y, Dept. of the Air Force*, 2005 WL 2738327 , *4 (N.D. Tex. Oct. 24, 2005) (listing acts that have qualified as intrusion); *see also, Schulman v. Group W Productions, Inc.*, 18 Cal.4th 200, 230 (Cal. 1998) (in California, invasion of privacy typically involves physical intrusion, eavesdropping, wiretapping, and spying). Names and addresses are not characterized "as 'private' and 'highly intimate or embarrassing facts about a person's private affairs, such that its publication would be highly objectionable to a person of ordinary sensibilities.'" *Johnson v. Sawyer*, 47 F.3d 716, 732 (5th Cir. 1995) (quoting *Industrial Foundation of the Industrial Foundation of the South v. Texas Industrial Accident Board*, 540 S.W.2d 668, 683 (Tex. 1976)); *Low v. LinkedIn Corp.*, No. 11–CV–01468–LHK, 2012 WL 2873847, *9 (N.D. Cal., Jul. 12, 2012) (disclosure of identity and browsing history not "highly offensive" for purposes of invasion of privacy).

Plaintiffs asked Twitter to "scan [their] contacts for people [they] already know on Twitter" (SAC ¶ 232.) Plaintiffs' grievance boils down to the assertion that Twitter retained address book information that it admittedly had permission to review. In these circumstances, plaintiffs cannot plausibly suggest an alleged "upload" of user contacts was "highly offensive" under the law.[8] Accordingly, the invasion of privacy claim against Twitter should be dismissed.

---

[7] Given the uncertainty in the SAC about which law applies to the common law claims, Twitter refers to California and Texas law, which do not materially differ for purposes of this motion.

[8] Courts also have held that "an action for intrusion upon one's seclusion exists 'only when there has been a physical invasion of a person's property or . . . eavesdropping on another's conversation with the aid of wiretaps, microphones, or spying.'" *Tomblin v. Trevino*, No. SA01CA1160-OG, 2002 WL 32857194, at *4 (W.D. Tex. June 17, 2002) (citing *Ross v.*

b. Theft

Plaintiffs fail to allege theft because they consented—in fact, affirmatively requested—that Twitter scan their contacts. *See* Tex. Penal Code § 31.03(a), (b) (requiring an unlawful act and defining "unlawful" to include appropriation "without the owner's effective consent"). Plaintiffs also do not claim that Twitter acted "with intent to deprive [Plaintiffs] of property," *see* Tex. Penal Code § 31.03(a), or that Twitter withheld data, required payment to restore data, or disposed of any data so that recovery by plaintiffs was unlikely. *See* Tex. Penal Code § 31.01(2) (defining "deprive"). Plaintiffs do not and cannot allege that Twitter took their contacts and they no longer have access to the data on their mobile phones. The Court should therefore dismiss plaintiffs' claims for theft and for liability under Tex. Civ. Prac. & Rem. Code § 134.001, *et seq*.

c. Conversion and Trespass to Chattels

As with theft, plaintiffs do not plausibly allege Twitter obtained access to their address books "in an unlawful and unauthorized manner," or that Twitter "wrongfully interfered" with those contacts, as needed to state claims for conversion and trespass to chattels, respectively. *See United Mobile Networks, L.P. v. Deaton*, 939 S.W.2d 146, 147 (Tex. 1997) (conversion requires access "in an unlawful and unauthorized manner"); *Bank of New York v. Fremont General Corp*., 523 F.3d 902, 914 (9th Cir. 2008) (conversion requires wrongful act); *Jon Jones v. Boswell*, 250 S.W.3d 140 (Tex. App.-Eastland 2008, no pet.) (wrongful interference required for trespass).

Plaintiffs also fail to allege that Twitter "exercised dominion and control" over the address book data "to the exclusion of" plaintiffs' rights, or that plaintiffs made a demand that Twitter refused to honor, as required for conversion. *See Nolte v. Flournoy*, 348 S.W.3d 262, 269 (Tex. App.-Texarkana 2011, pet. denied) (listing elements of conversion); *Zaslow v. Kroenert*, 29 Cal.2d 541, 551 (Cal. 1946) (same). Plaintiffs not only *asked* to have their contacts reviewed by Twitter, *they still have those contacts in their possession*. *See FMC Corp. v. Capital Cities/ABC, Inc*., 915 F.2d 300, 303-04 (7th Cir. 1990) (no claim for conversion where the defendant only has "a copy of the owner's property"). Plaintiffs further do not plausibly

---

Midwest Comm'ns, Inc., 870 F.2d 271, 273 (5th Cir. 1989)). Plaintiffs allege no such act and consented to Twitter reviewing their address books.

suggest their address book data was damaged, as required for liability to attach to a trespass claim. *Zapata v. Ford Motor Credit Co.*, 615 S.W.2d. 198 (Tex. 1981); *Intel Corp. v. Hamidi*, 30 Cal.4th 1342 (Cal. 2003) (trespass to chattels is not actionable without actual or threatened injury); *Jordan v. Talbot*, 55 Cal.2d 597,601 (Cal. 1961) (recovery requires actual damage).

Plaintiffs speculate that data aggregators might assign value to bulk contact lists and that defendants somehow reduced that value (SAC ¶ 77), but plaintiffs have not plausibly alleged that they ever intended to use their cell phone address books commercially. (SAC ¶ 78) (complaining about the loss of privacy of their data). Plaintiffs' contentions are even more illogical and implausible than those of a celebrity who asserts that use of his photograph disclosed a private fact *and* violated his right of publicity.

d. Computer Hacking, Cal. Penal Code § 502

Plaintiffs claim Twitter violated Cal. Penal Code § 502, a California statute that prohibits computer hacking. *See* Cal. Penal Code § 502(a). Section 502 contains several causes of action, and requires action "without permission," but this allegation has not been made against Twitter. A provider does not act "without permission" where, as here, it performs a service that a user requests. *See In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *12-13 (N.D. Cal. Sept. 20, 2011) (*In re iPhone I*) (holding service providers could not have acted without permission because plaintiffs voluntarily downloaded the software). Nor do plaintiffs allege Twitter bypassed or circumvented any technical barriers or restrictions, which courts have required to establish lack of permission under § 502. *See, e.g., Facebook v. Power Ventures*, No. C08-05780 JW, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010) (persons are only liable for acting "without permission" under § 502 if they "access[] or us[e] a computer, computer network, or website in a manner that overcomes technical or code-based barriers").

e. Negligence, Negligence *Per Se*, and Gross Negligence

Plaintiffs plead no facts showing Twitter owed a legal duty, as required to state a claim for negligence. (*See* SAC ¶ 327) (merely alleging that Twitter "breached the duty of care owed to Plaintiffs and [its] users"). *Kroger v. Elwood*, 197 S.W.3d 793 (Tex. 2006); *Texas Home*

Mgmt., Inc. v Peavy, 89 S.W.3d 30 (Tex. 2002) (duty requires complex consideration of the risk, foreseeability, and likelihood of injury weighed against the social utility of the conduct); *Romero v. Superior Court*, 89 Cal. App. 4th 1068, 1078 (Cal. App. Ct. 2001) (same). The SAC also fails to detail a specific injury resulting from the alleged breach. Plaintiffs' allegations of harm are "too speculative to support a claim for negligence" and "stem from disappointed expectations from a commercial transaction and thus do not form the basis of a negligence claim." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1064 (N.D. Cal. 2012) ("*In re iPhone II*"). "[D]iminished and consumed Apple Device resources, such as storage, battery life, and bandwidth;" "increased, unexpected, and unreasonable risk to the security of sensitive personal information;" and "disappointed expectations from commercial transaction" are insufficient to show "appreciable, nonspeculative, present injury" to state a negligence claim. *Id.*

Plaintiffs also allege no facts to establish that Twitter violated a statute designed to prevent injury to the class of persons to which plaintiffs belong, as required to state a negligence *per se* claim. *Moughon v. Wolf*, 576 S.W.2d 603, 604 (Tex. 1978); CAL. EVID. CODE § 669. Plaintiffs claim all defendants "violated criminal law and general standards of care," (SAC ¶ 326), but the facts contradict this claim: Twitter allegedly obtained address book information only after plaintiffs asked Twitter to scan their contacts (SAC ¶¶ 231-232), and only as described to plaintiffs in Twitter's Terms. This is consistent with the purported "industry standards" described by plaintiffs, which require "user consent" to obtain private information. (SAC ¶ 122.)

Finally, gross negligence cannot exist without a finding of ordinary negligence, *Hall v. Stephenson*, 919 S.W.2d 454 (Tex. App.-Fort Worth 1996, writ denied), and requires an additional showing, not present or even alleged here, that Twitter's actions involved an "extreme risk" of harm and were made with "conscious indifference" to the rights, safety, or welfare of others. *See Texas Dept. of Parks and Wildlife v. Miranda*, 133 S.W.3d 218 (Tex. 2004); *City of Santa Barbara v. Superior Court*, 41 Cal.4th 747, 754 (Cal. 2007) (gross negligence is a "want of even scant care" or "an extreme departure from the ordinary standard of conduct").

f. Common Law and Trade Secret Misappropriation

As is necessary to state a claim for common law misappropriation, plaintiffs do not allege facts that plausibly show that they created a "product through extensive time, labor, skill and money," that Twitter used "that product in competition" with plaintiffs, or that plaintiffs suffered "commercial damage." *Dresser-Randy Co. v. Virtual Automation Inc.*, 361 F.3d 831, 839 (5th Cir. 2004) (citing *U.S. Sporting Prods., Inc. v. Johnny Stewart Game Calls, Inc.*, 865 S.W.2d 214, 219 (Tex. App.-Waco 1993, writ denied). They make a conclusory statement that the defendants "secretly swept into their [systems] plaintiffs' private address books and used those materials for their own purposes and to their own benefit" but allege no facts against Twitter to support this claim. Nor do plaintiffs allege that Twitter used the information in competition with plaintiffs or that the information "confers on [plaintiffs] a commercial advantage" as required to show "a protectable property interest" for misappropriation in Texas. *U.S. Sporting Prods.*, 865 S.W.2d at 219. Plaintiffs also cannot plausibly allege appropriation or use without consent, as required to state a claim in California. *United States Golf Assn. v. Arroyo Software Corp.*, 69 Cal. App. 4th 607, 618 (Cal. App. Ct. 1999) (elements require plaintiff's investment of substantial time, skill or money; appropriation and use by defendant at little or no cost; defendant's appropriation or use without plaintiff's consent; and injury to plaintiff).

Further, plaintiffs alleged no facts showing their address book information constitutes a trade secret or proprietary information, for a "misappropriation of trade secrets" claim.[9] Such a claim requires "1) the existence of a trade secret; 2) breach of a confidential relationship or improper discovery of a trade secret; 3) use of the trade secret; and 4) damages." *Bohnsack v. Varco, L.P.*, 668 F.3d 262 (5th Cir. 2012). Plaintiffs fail to plead the first element, as their cell phone contacts are not "a process or device for continuous use in the operation of the business," nor does they "relate[] to the production of goods, as, for example, a machine or formula for the

[9] Misappropriation of trade secrets in California is a statutory claim, which Plaintiffs have not alleged. Nonetheless, the elements are not materially different from Texas law. CAL. CIV. CODE § 3426.1 *et seq*. (plaintiffs must own a trade secret, which defendants must be acquire, disclose or used improperly, and plaintiffs must be damaged).

production of an article." *Hyde Corp. v. Huffines*, 314 S.W.2d 763, 777 (Tex. 1958). Plaintiffs' speculative assertion that their contacts have economic value to individuals and took time to assemble (SAC ¶¶ 76-83) do not come close to pleading use of "secrets" relating to "trade."[10]

g. Unjust Enrichment

Unjust enrichment is a theory of recovery based on quasi-contract, not a cause of action. *Mowbray v. Avery*, 76 S.W.3d 663, 679 (Tex. App.-Corpus Christi 2002, pet. denied); *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1370 (Cal. App. Ct. 2010). It is unavailable where a "valid, express contract governing the subject matter of the dispute exists"—such as Twitter's Terms, which explain how Twitter collects and uses information. *Coghlan v. Wellcraft Marine Corp.*, 240 F.3d 449, 454 (5th Cir. 2001); *Paracor Finance, Inc. v. General Elec. Capital Corp.*, 96 F.3d 1151, 1167 (9th Cir. 1996). Moreover, plaintiffs fail to allege that Twitter "obtained a benefit" as required to recover under a theory of unjust enrichment, let alone that Twitter obtained this alleged benefit "by fraud, duress, or the taking of an undue advantage." *Heldenfels Bros., Inc. v. City of Corpus Christi*, 832 S.W.2d 39, 41 (Tex. 1992).

h. Constructive Trust

Constructive trust is not an independent cause of action. *Haber Oil Co. v. Swinehart (In re Haber Oil Co.)*, 12 F.3d 426, 436 (5th Cir. 1994) ("Under Texas law, a constructive trust is not actually a trust, but rather an equitable remedy imposed by law to prevent unjust enrichment resulting from an unconscionable act."); *Haskel Eng'g & Supply Co. v. Hartford Acc. & Indem. Co.*, 78 Cal. App. 3d 371, 375 (Cal. App. Ct. 1978) (constructive trust is "an equitable remedy"). A constructive trust would not be a proper remedy here, because plaintiffs cannot plead that Twitter was unjustly enriched. *In re Bradley*, 501 F.3d 421, 432 (5th Cir. 2007) (requiring "unjust enrichment" to support a constructive trust remedy).

---

[10] The SAC also lacks the necessary allegation of "use," as plaintiff cannot show an "exploitation of the trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant." *Gen. Universal Sys. v. HAL, Inc.*, 500 F.3d 444, 450 n.4 (5th Cir. 2007). Plaintiffs merely speculate that address book data generally has value for data aggregators and that plaintiffs suffered "damage" by its "de-privatiz[ation]"—but fail to include any plausible assertions of actual value and damage. Plaintiffs also fail to allege facts showing that Twitter used plaintiffs' contacts for any purposes other than to provide the matching service requested.

i. Wiretap Claims Under California and Texas Law

California Penal Code § 631 penalizes anyone that, "in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." In short, § 631 applies to the "(1) tapping the line, (2) making an unauthorized connection with the line, and (3) reading, attempting to read, or learning the contents or meaning of a message while the message is in transit." *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 898 (Cal. App. Ct. 1975). The offense can only occur when a *third party* listens in to what is said privately. *Id*. at 899. Plaintiffs do not allege this. Even assuming an interception, plaintiffs consented to Twitter's review of their contacts and the data could not have been obtained in an "unauthorized manner."

The Texas Wiretap Act, Texas Penal Code § 16.02, mirrors the federal Wiretap Act, discussed next, and courts look to the federal Wiretap Act when interpreting it. *Garza v. Bexar Metropolitan Water District*, 639 F. Supp. 2d 770, 775 (W.D. Tex. 2009) ("[T]he Texas Wiretap Act was fashioned after the Federal Wiretap Act. The Texas statute mirrors the federal statute in several respects and makes reference to it."). Any claims for interception, use, and disclosure under Texas law should be dismissed for the same reasons as plaintiffs' claims under federal law.

D. Plaintiffs Fail to Adequately Allege the Statutory Claims Under Federal Law

1. Electronic Communications Privacy Act ("ECPA")[11]

a. Plaintiffs have not alleged an interception

Information stored on a computer cannot be "intercepted" under the Wiretap Act because accessing stored information is not intercepting it contemporaneous with its transmission. *Steven Jackson Games, Inc. v. Secret Serv.*, 36 F.3d 457, 460-62 (5th Cir. 1994) (holding seizure of electronic communications stored on a computer hard drive is not an interception under the Wiretap Act); *see also Fraser v. Nationwide Mut. Ins. Co.*, 52 F.3d 107, 113 (3d Cir. 2003)

[11] Plaintiffs label this claim as arising under the Electronic Communications Privacy Act ("ECPA"). SAC ¶¶ 333-343. In 1986, ECPA amended the Wiretap Act, 18 U.S.C. §§ 2510, *et seq*. and the Pen Register and Trap and Trace Statute, 18 U.S.C. §§ 3121, *et seq*., and created the Stored Communications Act 18 U.S.C. §§ 2701, *et seq*. The Complaint cites 18 U.S.C. § 2520 as the source of the cause of action and parrots the Wiretap Act's language about interception, use, and disclosure, so Twitter treats this cause of action as arising under the Wiretap Act.

(holding access to electronic communications not "at the initial time of transmission" was not an interception); *U.S. v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003) (holding "contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (holding interception occurs when it "stop[s], seize[s], or interrupt[s] in progress or course before arrival"). Plaintiffs allege Twitter "uploaded all email addresses and phone numbers from the Apple Device owner's address book" (SAC ¶ 235); that is, that Twitter took stored information "from [their] [Apple Devices]" and "off of [their Apple Devices]" (SAC ¶ 233) or information that was "maintained" on their Apple Devices (SAC ¶¶ 2, 7, 44(v), 90, 183, 350, 369). Plaintiffs do not allege, as required to plead a wrongful interception, that Twitter stopped, seized, or interrupted transmission of this information.

b. Plaintiffs have not alleged use of an interception device, and any alleged interception would have been in the ordinary course of Twitter's providing its Find Your Friends feature

To scan plaintiffs' contacts to find friends already on Twitter with the "Find Your Friends" feature, Twitter must cross-reference them against data on Twitter's servers. This is the ordinary functioning of the matching service plaintiffs requested. But an unlawful interception under the Wiretap Act requires use of an interception "device," which excludes "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . furnished to the subscriber or user by a provider or a wire electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business." 18 U.S.C. § 2510(5)(a); *Hall v. Earthlink Network, Inc.* 396 F.3d 500, 503-04 (2d. Cir. 2005) (holding under § 2510(a)(5) that an Internet and email service provider that received emails sent to a closed email account in the ordinary course of the provider's business did not use a "device"). Despite an attempt to plead otherwise, Twitter's app—provided to Twitter users so they can use Twitter and the Find Your Friends service—cannot be such a device.

Additionally, an express exception to liability in the Wiretap Act allows an "officer, employee, or agent of a provider of wire or electronic communication service, whose facilities

are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of his service." 18 U.S.C. § 2510(2)(a)(i); *see U.S. v. New York Tel. Co.*, 434 U.S. 159, 168, n.13 (1977) ("all normal telephone company business practices [are excluded] from the prohibitions of the [Wiretap] Act."); *U.S. v. Savage*, 564 F.2d 728, 732 (5th Cir. 1977) (holding that the interception of a telephone conversation by a hotel owner who listened to a conversation between a caller and a hotel guest was permissible under section 2511(2)(a)(i)). Even assuming an interception, Twitter's "Find Your Friends" service necessarily must compare a user's contacts against data on Twitter's servers regarding other users. Without that ability, Twitter could not provide the matching that users ask it to do.

c. Plaintiffs have not alleged wrongful use or disclosure

While plaintiffs have completely failed to allege facts that would show Twitter used or disclosed the address book data outside of what plaintiffs consented to, any use or disclosure by Twitter of allegedly intercepted communications was lawful because using or disclosing intercepted communications violates the law only if the initial interception was unlawful. 18 U.S.C. § 2511(c), (d); *U.S. v. Turk*, 526 F.2d 654, 658-59 (5th Cir. 1976) (holding that section 2511(c) makes unlawful only the disclosure of "illegally intercepted" communications and listening to a recording of a conversation, where the initial recording was lawful, did not violate Wiretap Act); *see also Noel v. Hall*, 568 F.3d 743, 751 (9th Cir. 2009) (holding that sections 2511(c) and (d) "protect against the dissemination of private communications that have been *unlawfully* intercepted") (emphasis in original). Here, there was no interception, let alone an unlawful one, and without this predicate act, the claim for wrongful use or disclosure fails.

2. 18 U.S.C. § 1030(g), Computer Fraud and Abuse Act ("CFAA")

a. Plaintiffs have not alleged a specific claim under the CFAA

It is almost impossible for Twitter to address plaintiffs' attempt to plead a cause of action under the CFAA because plaintiffs have not identified which section or sections of the statute they believe Twitter violated. 18 U.S.C. § 1030(g) is the only section identified in the SAC, and

it merely authorizes civil actions and does not proscribe conduct. So Twitter is left to try to read plaintiffs' minds, cobble together the conclusory statements in SAC ¶¶ 344-35 and the rest of the SAC, and attempt to combat these non-specific allegations that could fall under several of the numerous types of conduct that are unlawful under the statute. *See* 18 U.S.C. §§ 1030(a)(1), (2)(A)-(C), (3), (4), (5)(A)-(C), (6)(A)-(B), (7)(A)-(C), (b). This basic pleading failure alone warrants dismissal of plaintiffs' CFAA claims. Fed. R. Civ. Proc. 8(a)(2); *Anderson v. U.S. Dept. of Hous. & Urban Dev.*, 554 F.3d 525, 528 (5th Cir. 2008) (under Rule 8, "defendants in all lawsuits must be given notice of the specific claims against them.")[12]

b. Plaintiffs have not sufficiently alleged a statutory prerequisite under Sections 1030(g) and 1030(c)(4)(A)(i)

The CFAA is primarily a criminal statute and civil actions are authorized only when there is loss aggregating at least $5,000 over a one-year period; actual or potential modification or impairment of a medical examination, diagnosis or treatment; physical injury to any person; a threat to public health or safety; or damage affecting certain sensitive computers used by the U.S. Government. 18 U.S.C. § 1030(g) and (c)(4)(A)(i)(I)-(V). The assertion that "Defendants . . . jeopardized public security and computers owned or used by the government in furtherance of justice, defense, or security" is ludicrous. (SAC ¶ 347.) And there is no mention of a modification to medical diagnoses or a physical injury, so the only potential basis for plaintiffs' claim is "loss" aggregating at least $5,000 over a one-year period.[13]

"Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other

[12] *See also Cenveo Corp. v. CelumSolutions Software GMBH & Co KG*, 504 F. Supp. 2d 574, 580 (D. Minn. 2007) ("A party cannot bring a civil action based on provisions other than § 1030(a)(5)."); *cf. Motorola, Inc. v. Lemko Corp.*, 609 F. Supp.2d 760 (N.D. Ill. 2009) (allowing civil action under § 1030(a)(4) but holding Rule 9(b) applies).

[13] That Congress grouped "loss" with physical injury, threats to public health and safety, impairment of medical diagnosis or treatment, and damage to federal government computers dealing with national security warrants an interpretation limited to "the traditional computer 'hacker' scenario where the hacker deletes information, infects computers, or crashes networks." *AtPac*, 730 F. Supp. 2d. at 1185; *see also In re iPhone II*, 844 F. Supp. 2d at 1065.

consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Damage is "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). A "loss" is therefore only two things: (1) a reasonable cost to a victim and (2) lost revenue or impairment to data, a program, system, or information incurred as a result of a service interruption. *AtPac, Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1184 (E.D. Cal. 2010). Plaintiffs hypothesize that transmission of address books "used [Apple Device] resources, battery life energy and cellular time, at a cost to the Plaintiffs, and . . . consumption of additional electricity purchased by Plaintiffs" (SAC ¶ 81), but this is a far cry from the statute's examples of responding to an offense, conducting a damage assessment, and restoring data, or a program, or system. *Cf. In re iPhone II*, 844 F. Supp. 2d at 1068 (holding that creation of files on a device that consumed the device's cache or gigabytes of memory and shortened the devices' battery life were not "damage"). In SAC ¶ 82, plaintiffs speculate they "are entitled" to have repairs made to their Apple Devices and have their data integrity validated, but they have not actually incurred these costs. Plaintiffs also have not alleged their service was interrupted. These conjectural injury allegations are the type courts have rejected. *See In re iPhone II*, 844 F. Supp. 2d at 1067-68 (collecting cases where courts have rejected that "personal information . . . constitutes economic damages under the CFAA"); *see also Cherny v. Emigrant Bank*, 604 F. Supp. 2d. 605, 608 (S.D.N.Y. 2009) (holding that release of an email address does not constitute injury and collecting cases establishing that "release of potentially sensitive information alone, without evidence of misuse, is insufficient to cause damage").

c. Plaintiffs have not alleged Twitter acted without authorization or exceeded authorized access

Plaintiffs have not pled that Twitter acted without authorization because they admit they asked Twitter to review their contacts for the Find Your Friends feature. *See LVRC v. Brekka*, 531 F.3d 1127, 1133 (9th Cir. 2009) (holding that giving permission to use a computer is authorization under the CFAA and a user therefore did not and could not act "without authorization" under the CFAA). Further, Twitter cannot have exceeded its authorized access to

the address book data because this is limited to unauthorized access to or alteration of data, not misuse or misappropriation (which is what plaintiffs apparently have tried to allege). 18 U.S.C. § 1030(e)(6) (defining "exceeds authorized access" as to "access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"); *U.S. v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (holding that the CFAA targets unauthorized procurement or alteration of information, not its misuse or misappropriation); *cf. U.S. v. John*, 597 F.3d 263, 273 (5th Cir. 2010) (holding that exceeding authorized access does apply to misuse, but only where the "user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime").

E. Plaintiffs Have Failed to Adequately Allege the RICO Claim

The RICO civil cause of action is "for those injured in their business or property by a violation of RICO's criminal prohibitions, and in an effort to combat organized, long-term criminal activity." *Ausley v. Cross Country Water Supply Corp.*, No. A-09-CA-660-SS, 2010 WL 5647119, *7 (W.D. Tex. April 16, 2010) (quoting *Jennings v. Auto Meter Prods., Inc.*, 495 F.3d 466, 472 (7th Cir. 2007)). "[T]he statute was never intended to allow plaintiffs to turn garden variety state law fraud claims into federal RICO actions." *Ausley*, 2010 WL 5647119, at *7 (quoting *Jennings*, 495 F.3d at 472). Plaintiffs attempt to do just that by accusing Twitter of being part of a scheme in which multiple competing companies conspired to "mak[e] money" and "gain[] market share" by "distribut[ing] malware to millions of consumers' [Apple Devices] and turn[ing] them into zombie bots." (SAC ¶ 362.) The allegations are simply implausible and fail to include the elements of a RICO civil claim: "1) a *person* who engages in 2) a *pattern of racketeering activity*, 3) connected to the acquisition, establishment, conduct, or control of an *enterprise*." *Delta Truck & Tractor, Inc. v. J.I. Case Co.*, 855 F.2d 241, 242 (5th Cir. 1988).

First, plaintiffs fail to plead non-speculative facts showing a "concrete financial loss" or "an actual loss 'of their own money,'" as necessary to have standing to bring a RICO claim. *In re Taxable Mun. Bond Sec. Litig.*, 51 F.3d 518, 523 (5th Cir. 1995) (internal citation omitted).

Plaintiffs also allege no facts against Twitter that would support the first two elements of a RICO claim. "Racketeering activity" involves two or more related predicate criminal acts and "amount to or pose a threat of continued criminal activity." *Id.* Plaintiffs' allegations, however, show only that Twitter provided users with a requested service, a far cry from Congress's "concern in RICO with long-term criminal conduct." *H.J. Inc. v. Nw. Bell Telephone Co.*, 492 U.S. 229, 242 (1989). Plaintiffs also fail to "state with particularity the circumstances constituting the fraud," as required for fraud-based RICO claims under Fed. R. Civ. P. 9(b).[14]

Nor do plaintiffs sufficiently allege the three "structural features" of an enterprise in fact: "purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose." *Boyle v. U.S.*, 129 S. Ct. 2237, 2244 (2009). Plaintiffs do not allege any facts showing why or how any defendants participate or benefits in an enterprise, and they fail to explain how more than a dozen competitors work together to "gain market share." Further, plaintiffs incorrectly allege that Twitter is both a person under § 1962(c) and a member of the purported enterprise-in-fact (*see* SAC ¶ 362), but "a RICO person cannot employ or associate with himself under this subsection." *In re Burzynski*, 989 F.2d 733, 743 (5th Cir. 1993); *see also, Crowe v. Henry*, 43 F.3d 198, 205 (5th Cir. 1995) (dismissing RICO cause of action because plaintiff alleged defendant "is both the RICO person and a member of the [alleged] association-in-fact").

Alternatively, plaintiffs fail to allege facts establishing that defendants "have an existence separate and apart from the pattern of racketeering, are an ongoing organization, and function as a continuing unit as shown by a hierarchical or consensual decision making structure." *Brunig v. Clark*, 560 F.3d 292, 297 (5th Cir. 2009). The only connection alleged among Twitter and other defendants is that the apps are distributed through Apple's App Store for use on Apple Devices, and all the defendants share the desire to make money. That is not a RICO conspiracy.

[14] Twitter also refers to and adopts the additional arguments and authorities presented by other defendants regarding plaintiffs' failure to comply with the pleading requirements of Rule 9(b).

F. This Court Should Dismiss Plaintiffs' Action Pursuant to Rule 12(b)(3) or 12(b)(1)

Twitter should also be dismissed[15] as a defendant under Rule 12(b)(3) or 12(b)(1).[16] "[F]orum selection clauses are prima facie valid and should be enforced unless enforcement is shown by the resisting party to be unreasonable under the circumstances, and that courts should enforce such clauses unless the resisting party could clearly show that enforcement would be unreasonable and unjust, or that the clause was invalid for such reasons as fraud or overreaching." *Int'l Software Sys., Inc. v. Amplicon, Inc.*, 77 F.3d 112, 114 (5th Cir. 1996), citing *M/S Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1, 10 (1972). *See also Ambraco*, 570 F.3d at 243 ("A valid forum-selection clause renders venue improper in the non-designated forum, even if the non-designated forum would otherwise be proper.").[17]

Twitter's Terms, accepted by plaintiffs, govern "all claims, legal proceedings, and litigation arising in connection with the Services," and apply to the SAC. (Kim Decl., ¶ 8, Exs.

---

[15] Dismissal is the appropriate remedy here. *Int'l Software Sys., Inc. v. Amplicon*, 77 F.3d 112, 115 (5th Cir. 1996) (affirming this Court in holding dismissal is proper based on forum selection clause); *see also* 28 U.S.C. § 1406(a) (dismissal required when case filed in wrong venue unless the interests of justice require transfer). Furthermore, the Court should dismiss because the clause allows plaintiffs to choose between the federal or state courts in California. *Rassoli v. Intuit, Inc.*, No. H-11-2827, 2012 WL 949400, at *4 (S.D. Tex. Mar. 19, 2012). Dismissal is also appropriate because Twitter should be severed from this action. *See* Twitter's concurrently-filed Motion to Sever. Plaintiffs may argue that this Court should apply 28 U.S.C. § 1404 to the question of proper venue, but this is inconsistent with *Amplicon*, *Haynsworth*, and *Ginter*, cited *infra*, as § 1404 "addresses the proper analysis for determining motions to transfer venue, not for determining motions to dismiss." *VarTec Telecom, Inc. v. BCE Inc.*, No. 3:02-cv-2585-M, 2003 WL 22364302, at *6 (N.D. Tex. Oct. 9, 2003). If the Court analyzes venue under § 1404(a), however, Twitter should be severed and any surviving action transferred to the Northern District of California. When a § 1404 motion relies on an enforceable forum selection clause, the clause should be enforced absent exceptional circumstances not present here. *See, e.g.*, *Marinechance Shipping, Ltd. v. Sebastian*, 143 F.3d 216, 220, n.16 (5th Cir. 1998) (internal citation omitted). Even a traditional analysis of the §1404(a) factors should result in transfer to the Northern District of California. *In re Volkswagen AG*, 371 F.3d 201, 203 (5th Cir.2004). The majority of documents and witnesses are in California. (Kim Decl., ¶ 12). Some plaintiffs are not located in Texas and have accepted any slight inconvenience for representing a putative national class in an action litigated outside their state. (SAC ¶¶ 5-18). Moreover, California law may govern some of plaintiffs' claims against Twitter and the Complaint alleges causes of action under California law, so the public interest factors weigh in favor of transfer or are at least neutral. Finally, plaintiffs' choice of forum is given little weight when the case is a putative national class action. *In re Triton Ltd. Sec. Litig.*, 70 F. Supp. 2d 678 (E.D. Tex. 1999); *Broadhead Ltd. P'ship v. Goldman, Sachs & Co.*, No. 2:06-CV-9, 2007 WL 951511, at *1 (E.D. Tex., Mar. 28, 2007).

[16] There is some uncertainty in the Fifth Circuit whether a motion to dismiss for improper venue falls under Rule 12(b)(1) or Rule 12(b)(3); the standards are the same. *Ambarco, Inc. v. Bossclip B.V.*, 570 F.3d 233, 237-8, n.1 (5th Cir. 2009) (citation omitted).

[17] In the Fifth Circuit, federal law governs the enforceability of forum selection clauses. *Ginter ex rel. Ballard v. Belcher, Prendergast & Laporte*, 536 F.3d 439, 441 (5th Cir. 2008).

D-I). Each claim against Twitter arises from the use of its services, in particular its application on Apple Devices and the incorporated "Find your Friends" feature. (SAC ¶¶ 231-237); *Ginter ex rel. Ballard v. Belcher, Prendergrast & Laporte*, 536 F.3d 439, 444-45 (5th Cir. 2008) (courts "examine[] the language of [a] forum selection clause with a common-sense view of the causes of action to determine whether the clause was broad enough to cover [the causes of action]").

"The party resisting enforcement on these grounds bears a 'heavy burden of proof.'" *Haynsworth v. The Corp.*, 121 F.3d 956, 963 (5th Cir. 1997) (quoting *M/S Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1, 17 (1972)); *Ginter Haynsworth ex rel. Ballard*, 536 F.3d at 441 ("Under federal law, forum-selection clauses are presumed enforceable, and the party resisting enforcement bears a heavy burden of proof."); *Bizware Software Solutions, Inc. v. Groupe Conseil Gabriel Amar et Associes Inc.*, No. 1:11-cv-00316-ss, at *8 (W.D. Tex. Aug. 8, 2011) (quoting *Ginter*). Plaintiffs can meet this burden only by showing the clause is "unreasonable" under circumstances including fraud, grave inconvenience, fundamental unfairness, or public policy. *Lighthouse MGA, L.L. C. v. First Premium Ins. Grp., Inc.*, 448 F. Appx. 512, 514 (5th Cir.2011) (per curiam) (internal quotation marks omitted) (quoting *Haynsworth*, 121 F.3d at 963). Plaintiffs have not and cannot allege such facts and the Court should therefore dismiss this action with respect to Twitter.

IV. CONCLUSION

For the reasons above, Twitter respectfully requests that this Court dismiss all claims against Twitter and this action for lack of standing, failure to plead a claim, and improper venue.

DATED October 12, 2012

RESPECTFULLY SUBMITTED,

s/ Tanya D. Henderson
Tanya D. Henderson
State Bar No. 50511706
PERKINS COIE LLP
2001 Ross Avenue, Suite 4225
Dallas, Texas 75201-2904
Tel: 214.965.7700
Fax: 214.965.7799
thenderson@perkinscoie.com

s/ Timothy L. Alger
Timothy L. Alger (*admitted pro hac vice*)
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304
Tel: 650.838.4300
Fax: 650.838.4350
talger@perkinscoie.com

s/ Amanda J. Beane
s/ Ryan T. Mrazik
Amanda J. Beane (*admitted pro hac vice*)
Ryan T. Mrazik (*admitted pro hac vice*)
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Tel: 206-359-8000
Fax: 206-359-9000
abeane@perskincoie.com
rmrazik@perkinscoie.com

CERTIFICATE OF SERVICE

On October 12, 2012, I electronically submitted the foregoing document with the Clerk of Court for the United States District Court, Western District of Texas, using the electronic case filing system of the Court. I hereby certify that I have served all counsel for parties of record electronically or by another manner authorized by Federal Rule of Civil Procedure 5(b)(2) and Local Rule CV-5(b)(1).

DATED: October 12, 2012

s/ Amanda J. Beane
Amanda J. Beane